STRATEGY EBOOK SERIES

Smart Energy

IoT Device Management & Security in Product Strategy

Brought to you by
OTA software updates solution for IoT devices

MENDER

Get in touch: **contact@mender.io**

Northern.tech

8.5%

The proportion of Enterprise IoT devices **that could fail** in the field over 3 years without robust updating [1]

Reader ROI

The key summary points you should take away from this strategy ebook:

- Invest in a relationship with a Best of Breed technology partner to look after your IoT device infrastructure
- Understand that device management and security is the foundation for success: don't risk a security breach or embedded devices failing
- Be aware that Governments are mandating that basic security standards be built into IoT devices
- Invest in product extensibility so you can "unlock features" for your customers in the future, build subscriptions and recurring revenue streams
- And remember to stay flexible by avoiding vendor platform lock-in

Get in touch: **contact@mender.io**

Better Build the House of Bricks

Achieving business value from digital goes hand in hand with IoT device management and security.

In this strategy ebook, we lay out the best path for IOT and product management leaders to follow.

It goes without saying that energy providers and smart energy system integrators need to have a great strategy in place for IoT gateway device management and security.

This has implications for security, compliance with government regulations, and for the robust maintenance of new digital products built around over-the-air software updates.

Let's begin with a short analogy to highlight the key points...

"Let me in or I'll huff and I'll puff and I'll blow your house down." From childhood, we remember the Big Bad Wolf and how one little pig was better prepared than his brothers because he took the time to look after the construction of his house properly.

This story should not be lost on service providers in the smart energy industry who must build robust houses made from bricks too! What we mean by this analogy is that to deliver valuable digital connected products and services device management and security must constitute the foundation.

Device management and security can easily be perceived as costs to the business. As a result, the marching order is to minimize costs, and build the device infrastructure within the organisation cheaply. To build houses made of straw so to speak.

Chief Product and Innovation Officers such as Bjorn Nostdahl from security provider **Gunnebo** has already warned of the hassle and lost opportunity cost that comes from trying to build homegrown infrastructure such as software updating.[2] Service providers should resist this temptation at all costs and go for best-of-breed solutions instead!

Great value propositions depend on security and device management

As a Head of IOT or product manager you will want:

- Robust and secure device management and security to enable the execution of your business strategies.

- And to reduce the time and resources it takes to go from development to production for new features, and bring down the cost of shipping the software.

- You will also want to differentiate your proposition through doing things like “unlocking features” for customers in different subscription plans for their product. IoT offers a great opportunity to enable *subscription models* and *recurring revenue*.

Customers expect more from digital products with subscription models

However, the customer expects more out of a subscription than from one a one-time payment. They expect continuous product improvements, cloud services and instant support for the problem with the product. Device management is the key enabler for this.

Feature enhancements must be delivered in a robust and secure way. What if there is a long lead time between when the product leaves the factory and the point at which the customer opens the product for the first time? Will the product update as it should to the latest software version at launch? Will the current product version be compatible with your latest cloud/backend version? If not, will there be customer disappointment and a cost to the business to resolve the issue.

Often, software version upgrades need to be done in increments where the update knows the exact version and the upgrade path so without some automation, this might be very difficult to achieve after the event. An over the air software update needs to be built into the product strategy so there is an easy way for the user to get the required update.

The bottom line is that device management is a key strategic consideration and should be at the forefront of your considerations, and not be a costly afterthought.

Governments mandate security measures

Security is an integral part of device management for digital product providers. It is a must and there are a growing number of standards to adhere to.

Governments are constantly reminding the private sector of the threats and their responsibilities of services providers to protect consumers and businesses from device tampering and malicious threats.

As recently as October 22nd, 2020, Lucian Niemeyer, Deputy Program Director, National Security Programs, The White House noted "What can a virtual command do within a building or a piece of physical infrastructure to cause catastrophic damage or to threaten lives. Cyber criminals can turn a thermostat into a listening device or infrastructure against us."[3]

Signed into law, the landmark **Internet of Things ("IoT") Cybersecurity Improvement Act (H.R. 1668)** which firmly puts the onus on vendors to build the basc levels of security into their IOT products.[4]

German regulator makes security & privacy mandatory for Smart Energy Gateways

From Germany, we can look at the **Smart Energy Gateway meter roll out certified by the BSI (Bundesamt für Sicherheit in der Informationstechnik).** Regulation is used to hammer home the need to apply security to digitalisation.

The going isn't always smooth though. We know the security requirements in the certification are so stringent that the **Maleficent Queen** from the **Grimm Fairytale** looks less stern in comparison. Leading experts such as BNE (Association of Energy Market Innovators) have complained how **"tremendously high expectations regarding the safety and security of the intelligent metering systems were transferred from the politicians to the implementing authorities."** .[5]

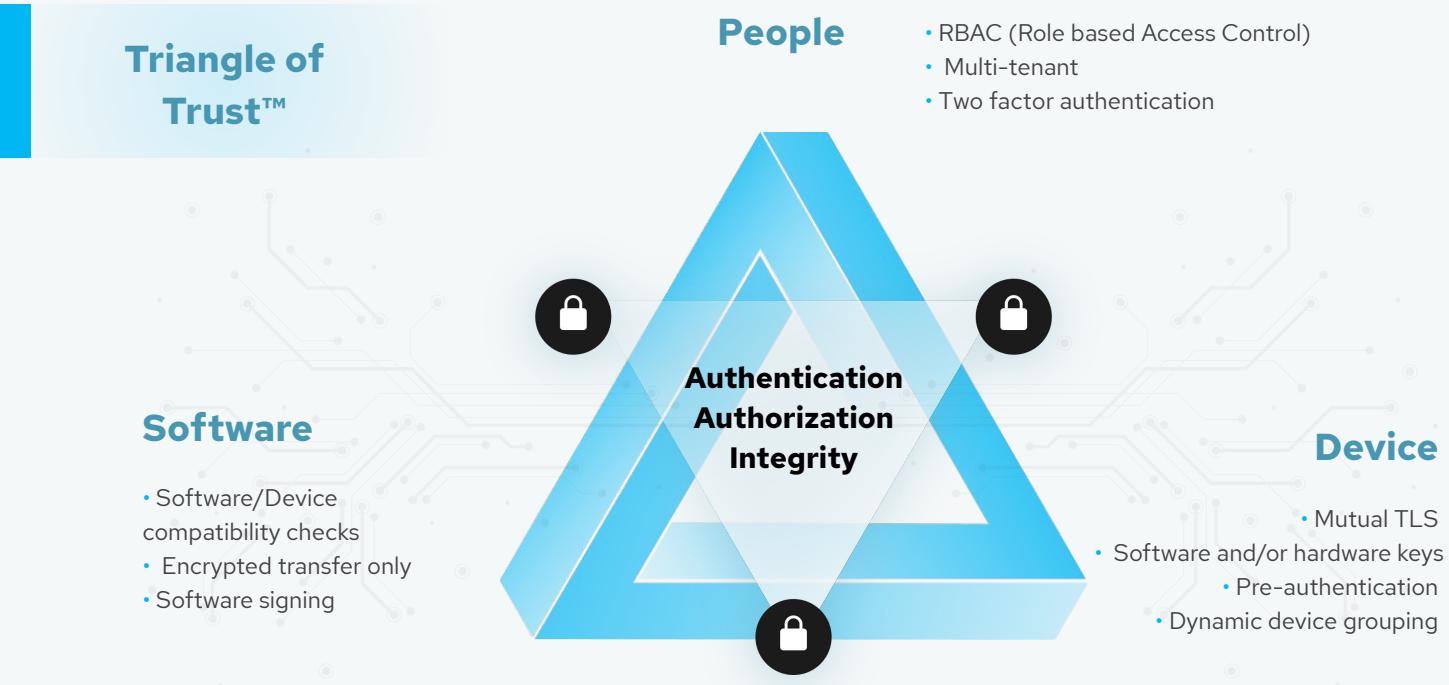
So security can be complex and tedious for service providers to address but it must be done. Selecting a partner who can manage the security requirements as part and parcel of the device management is the way forward. McKinsey notes **"the preferences of IoT leaders suggest a greater willingness to draw capabilities from an ecosystem of technology partners, rather than rely on homegrown capabilities."**.[6]

Look for a partner that puts security first

Consider a partner who advises you to incorporate the **Triangle of Trust™** into your device management and security strategy.

> *Only **authorised people** can deploy **authorised software** to **authorised devices.***
>
> *Which leads to*
>
> *Only the **right people** deploying the **right software** to the **right devices***

To realise the **Triangle of Trust™,** the partner must deploy the correct technologies to apply end to end security for the software and hardware to implement the policy.



Smart IOT leaders add smart features

A smart IOT leader will focus their plan on applying smart versions of their products to create business value by delighting their customers with new features. These could be great product enhancements. To succeed it is important to involve the right partners to manage their devices and security. Our customers **GridX** and **Northvolt** are examples of these types of software-smart organisations.

GridX helps homeowners better manage their energy consumption. A gateway management device collects data from PV panels, heat pumps and EV charging stations. It submits this data to a cloud platform for analysis so the insights can be used to optimise energy usage in the home. The company also provides a gateway management device enables EV charging station providers to better load balance energy consumption across "power hungry" fleets of charging stations. The gateway devices in both cases are being kept securely updated and have new software and security patches installed through an over-the-air updating process.

GridX wants to use its internal resources to keep developing their core product to the most important energy management use cases. Northern.tech's solution Mender is helping GridX with OTA software updates. **GridX CTO Joel Hermanns** points out that **"automatic updates roll back in cases of (device) power loss, would be difficult to replicate for GridX engineers to create internally. Mender just works from the get go and is really well designed."**

Ensuring remote access & software integrity

Northvolt also addresses the security and device management issues to give it a strong foundation to grow its business. Both its CEO and CTO cut their teeth at **Tesla** so it's only natural then that the company believes in secure remote updating of its products.

Northvolt manufactures large lithium-ion battery systems used to power heavy machinery. It uses the strong foundation of IOT and AI to get insights from data to help inform iterative product design and improvement.

The company uses a system of micro-controllers, edge devices and an AI- enabled cloud platform to take data from the field on the performance of battery cells and send key insights from it to their engineers in global R&D. **These insights help them better understand the battery cells and improve product performance at a better price for their customers.**

To transmit the data, **Northvolt** needs to ensure the gateway devices are working as expected with integrity. The delivery of Over-The-Air firmware and software updates ensures this. If a device does go offline, local software updates can be still be done securely. To enable this, **Mender** provides **Northvolt** with what are called "code signed" update artifacts. These artifacts which are wrappers with all the elements needed for a correct software update, have been reviewed and approved by the global HQ team. They can then be applied securely by a local engineer in the field.

And what about robustness?

Once deployed, devices should run smoothly in the background so the customer experience is never adversely affected.

There have been horror stories of "bricked" gateway devices creating financial loss and brand damage for the providers affected by it. A **botched firmware upgrade bricked over 500 door locks in apartments which had to be removed and replaced.** It took more than 18 days for maintenance work to be done to remove the affected locks.[7]

A robust device management solution would use automatic roll backs to previous software versions to avoid device bricking.

This is enabled through Mender's A/B partition design with automatic roll back to the previous software versions in event of power failure or connection loss. The updates should also be atomic so that there is no risk that a faulty library in a package could corrupt an update.

Wrapping up

In conclusion, **“the house made of bricks”** is the best investment. It is one that marries a focus on business value with superior security – **the Triangle of Trust™** – and device management.

The smartest Heads of IoT and product managers are aware of the need to find a trusted partner to help them take care of essential aspects of the foundation such as secure software updates.

Then they can focus on embracing digital to enhance their business to win more profitable customers and attain greater market share.

I think I saw a huntsman chasing a wolf in the distance.

Get in touch: E-mail contact@mender.io

References

1. Modelled data research from the Mender Product Management team

Based on quantitative field data, more than 8.5% device updates failed for any reason and would very likely have caused stability issues, unknown states or bricks if a robust update process like Mender was not utilized.

2. Bjorn Nostdahl personal blog on Mender and OTA software updates

https://tinyurl.com/y497ee8c

3. Keynote from IIOT World's Industrial Cybersecurity Day

https://tinyurl.com/y2abr2qx

4. Internet of Things ("IoT") Cybersecurity Improvement Act (H.R. 1668)

https://tinyurl.com/y54h58q3

5. BNE Position Paper on Smart Meter Roll-out in Germany

https://tinyurl.com/y4toax7q

6. Mckinsey & Company, "What separates leaders from laggards in the Internet-of-Things (2019)

https://tinyurl.com/y5r3wyr5

7. Bleepingcomputer.com

https://tinyurl.com/y6dxamxh